NOTICE OF PRIVACY PRACTICES (SUMMARY)

THIS NOTICE DESRCIBES HOW YOUR PROTECTED HEALTH INFORMATION MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.

This Notice describes the obligations of the Department of Employee Insurance (DEI) and your legal rights regarding your Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other things, this Notice describes how your PHI may be used or disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law. This is a summary of DEI's Notice of Privacy Practices. For complete information about DEI and KEHP's HIPAA Privacy and Security, please go to our web site at http://personnel.ky.gov/dei/hipaa.htm or call our Member Services Branch at 888-581-8834.

The Kentucky Employees' Health Plan (KEHP) is a self-funded governmental plan and, therefore, we are required to provide this Notice of Privacy Practice to you pursuant to HIPAA. DEI is the plan sponsor.

The HIPAA Privacy Rule protects only PHI. Generally, PHI is individually identifiable health information, including demographics information, collected from you or created or received by a health care provider, health care clearing house, or your employer on behalf of a group health plan that relates to: 1) your past, present, or future physical or mental health or condition; 2) the provisions or health care to you; or 3) past, present, or future payment for provisions of health care to you. **DEI does not maintain information regarding your specific medical condition but does maintain PHI related to demographic information and other information that is necessary for determining eligibility and enrollment in the KEHP**. If you have any questions about this Notice or about our Privacy Practices, please visit http://personnel.ky.gov/dei/hipaa.htm or contact Department of Employee Insurance, Attn; HIPAA Privacy Officer, 501 High Street, 2nd Floor, Frankfort, Kentucky 40601.

The effective date of this Notice is January 1, 2010.

DEI Responsibilities

We are required by law to: 1) maintain the privacy of your PHI; 2) provide you with certain rights with respect to your PHI; 3) provide you with a copy of this Notice of our legal duties and privacy practices with respect to your PHI; 4) follow Breach accounting and notification requirements; and 5) follow the terms of the Notice that is currently in effect. We reserve the right to change the terms of Notice and to make new provisions regarding your PHI that we maintain, or as required by law.

How DEI May Use and Disclose Your Protected Health Information

Under the law, we may use or disclose your PHI under certain circumstance without your permission. The following categories represent the different ways that we may use or disclose your protected health information: 1) **For Treatment;** 2) **For Payment;** 3) **For Health Care Operations;** 4) **To Business Associates;** 5) **As Required by Law;** 6) **To Avert a Serious Threat to Health or Safety;** 7) **To Plan Sponsors.**

Special Situations

In addition to the above, the following categories represent other possible ways we may use and disclose your PHI. 1) organ tissue donation, 2) military and veterans; 3) workers' compensation; 4) public health risk; 5) health oversight activities; 6) lawsuits and disputes; 7) law enforcement; 8) coroners, medical examiners and intelligence activities; 9) inmates; and 10) research.

Required Disclosures

DEI is required to disclose your PHI to you (as a participant) and for Government audits.

Other Disclosures

Other disclosures may be made to your personal representatives, spouses and other family members and with written authorization. DEI's HIPAA Forms may be located at http://personnel.ky.gov/dei/hipaa.htm.

Participant Rights

A participant has the following rights with respect to their PHI: 1) right to inspect and copy; 2) right to amend; 3) right to an accounting of disclosures; 4) right to request restrictions; 5) right to request confidential communications; and 6) right to a paper copy of this Notice.

Breach defined

The Breach Regulations provide a specific definition of "breach" for purposes of the notice obligations. Compliance with the Breach Regulations hinges on understanding this definition and being able to identify "breaches." A "breach" for purposes of the Breach Regulations and the corresponding notice obligation occurs only if (i) there is an acquisition, access, use or disclosure (ii) of unsecured PHI (iii) that violates the HIPAA Privacy Rules relating to use and disclosure of PHI and (iv) that compromises the security or privacy of the unsecured PHI. The definition of "breach" has several moving parts and exceptions. Therefore not every violation of the HIPAA Privacy Rules will constitute a breach for purposes of the Breach Regulations.

Breach Notification Requirements

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, U.S. Department of Health & Human Services (HHS) and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

1) Individual Notice

DEI shall notify affected individuals following the discovery of a breach of unsecured protected health information. DEI shall provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If DEI has insufficient or out-of-date contact information for 10 or more individuals, the Administrator must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the Administrator has insufficient or out-of-date contact information for fewer than 10 individuals, the Administrator may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Administrator is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Administrator.

2) Media Notice

When the Administrator experiences a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, it shall provide notice to prominent media outlets serving the State or jurisdiction. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

3) Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a

breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the Administrator may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

4) Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the Administrator following the discovery of the breach. A business associate must provide notice to the Administrator without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the Administrator with the identification of each individual affected by the breach as well as any information required to be provided by the Administrator in its notification to affected individuals.

Business Associates

Effective February 17, 2010, business associates are required to fully implement the information security safeguards specified by the HIPAA Security Rule. Additionally, pursuant to the HITECH Act business associates must implement written, comprehensive information security programs that address each aspect of the HIPAA Security Rule. Business Associates shall work with the Administrator in pursuit of Breach accounting and notification requirement established by the HITECH Act.

Complaints

If you believe that your privacy rights have been violated, you may file a complaint with DEI or with the Office of Civil Rights of the United States Department of Health and Human Services, electronic mail address: OCRMail@hhs.gov. To file a complaint with DEI please visit http://personnel.ky.gov/benefits/dei/hipaa.htm. All complaints must be in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office of Civil Right or with DEI.